Modified AODV Algorithm using Data Mining Process: Classification and Clustering

[1]Srivastava Sumit (Dr.), [2]Maheshwari Shashikant

[1]Associate Professor, Department of Computing and Information Technology, Manipal University Jaipur

[2]M.Tech Scholar- NIS, Department of Computing and Information Technology, Manipal University Jaipur

Mail-id: [1]sumit.srivastava@jaipur.manipal.edu, [2]lavish8@gmail.com

Abstract: - **Security of Wireless Ad hoc network has a primary concern to provide protected communication between mobile nodes. When we routing some packet it can use both malicious node or authenticate node for forwarding and receiving data. Malicious node can attack like black hole, misuse of data or hacked information. Our aim is to discuss the feasibility of monitoring the node of different networks, to analyze it for providing better security in AODV routing protocol. We implement data mining techniques for search large amount of data according characteristic rules and patterns to detect malicious node. We have used growing neural gas (GNS) clustering algorithm to make clusters and analysis data. Using soft computing technique we find patterns, analysis node and take decision based on decision tree.**

Keywords: - **Mobile Ad- hoc Network, AODV Routing protocol, Black hole attack, learning technique.**

I. Introduction

An ad hoc network is a self-configuring network of Wireless mobile nodes (router) without fixed infrastructure and centralized administration. They can communicate with multi-hop paths without access point and form arbitrary topology. Mobility is advantage for Ad-hoc network, Routers is free to move randomly, connect network environment transmits and receive data accordingly. Ad-hoc networks are very flexible, easily nodes can join and leave from network. Mobility of mobile node gave result in dynamic topology that makes highly vulnerable to security attacks and this is one main challenge of developers to develop secure Ad-hoc network [1].

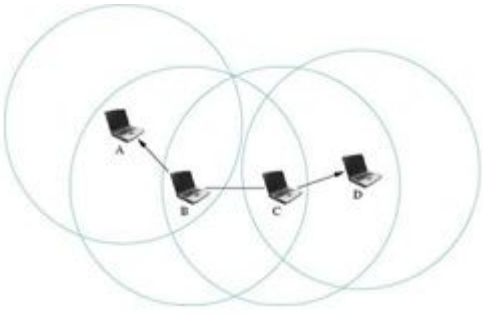

Fig 1: Circuit Explaining Ad-Hoc Networks

Generally we considered security of network we examine it under availability, integrity, confidentiality authentication and non-repudiation. Availability Ensure that the network is survivable and remain available at all times. Integrity says that a packet being transferred is never corrupted. Confidentiality, certain information is never disclosed to unauthorized entities Authentication Enables a node to ensure the identity of the peer node that it is communicating with. Non-repudiation, states that sender of massage never deny sent [2].

Developing secure ad hoc routing, Security is a serious issue, Due to absence of infrastructure ad hoc network, Routing protocol vulnerable to attacks such as Black Hole Attack, Grey Hole Attack, and Flooding Attack. Due to security vulnerabilities against attacker very difficult to determine malicious nodes which drops packets in network, if more than one malicious node are available in communication path they will support to each other to perform attack. For detection of malicious activity we proposed growing neural gas algorithm which will identified activity of intruders and based on decision tree we will take decision [12].

The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize efficiency. To detection of intruder's activity we proposed method using clustering algorithm easily identified attacks in network.

The rest of the paper is organized as Section II background, section III related work. Section IV proposed solution, V Section simulation VI conclude the paper.

II. Background

A. Ad-Hoc On Demand Distance Vector

There are three types of routing protocols: Proactive protocols, Reactive Protocols and Hybrid Protocols. Ad-hoc on demand distance vector (AODV) is a reactive protocol that doesn't require periodic advertisement. It enables maximum sequence number and minimum hop count dynamically maintain route table for intermediate nodes. AODV never falls in loop because it is based on sequence number that is serving as time stamps maintain latest information about intermediate node. Main advantage of AODV is least congested in minimum hop count [6].

B. Types of Attack on Aodv

There are two kinds of attack possible in AODV routing protocol passive attacks or active attacks. Passive attack

DOI: 03.LSCS.2013.3.35

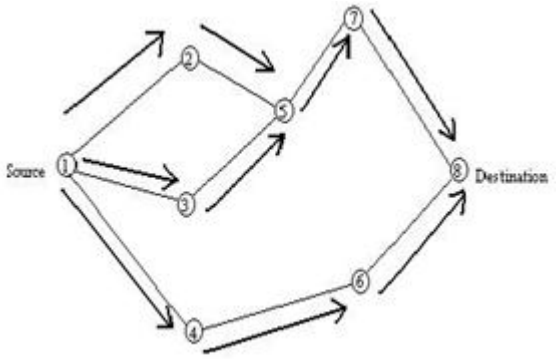

Fig 2: Diagram Explaining RREQ Packet traversing

sneaks data without modification network operation therefore difficult to detect. Active attack does modification, fabrication. Some of those discussed here:

Black hole attack: Black hole attack is one type of Distributed Denial of Service attack. In black hole attack malicious node injecting itself with minimum hop count in RREP during route discovery when source sends control packet to malicious node even route is spurious. In black hole attach malicious node can intentionally intercept packet without forward it. There is one more form of attack can possible when attacker send selective packets it can modified other packets which is forward by other intermediate node When a group of malicious nodes are supporting to each other than condition will become worst [3].

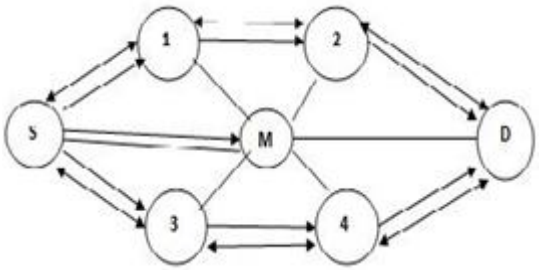

Fig 3: Diagram Explaining Malicious node

Gray hole attack: - It is variation of black hole attack, malicious node send RREQ packet as having valid route with minimum hop count to destination. When sender will send packet, it forwards most of them but may drop packets coming from destination or some specific node. Sometime behaviour as normal some time may combine behaviours of attacker. These types of attacks very difficult identify. [4].

Flood Attack: - Ad-hoc network often deploy in such environment where nodes have no physical protection against unattended tempering, and Distributed Denial of services (DDos). There are three types DDos attacks possible flood attack, protocol attack, and logical attack. In this paper we will only discuss about flood attack.

In AODV intruder broadcast so many fake Route Request packet to consume bandwidth and resources of network and own define sequence number to make attack more dangerous. Due to impact of DDos attack our security will compromise in Availability. Flood attack also increase congestion on Adhoc network [5].

C. Data Mining Techniques

Data mining can be viewed as an analysis of available information. Classification can be based on huge amount of data record. Clustering analysis algorithm can be used for partitioning a set of data object into subsets to check weather normal or intrusion behaviour. Clustering is a partitioning technique which divides the datasets into groups of M clusters.

The goal of clustering is to group sets of objects in the same cluster, while dissimilar objects are in separate clusters. Clustering can be used as analysis and store information about node, pattern recognition and supervised learning. Any cluster should exhibit two main properties low inter-class similarity and high intra-class [7].

We proposed Neural- Gas clustering algorithm for comprehensive learning technique. In which multiple centroids update whenever data information is added. Update depends on distance between data object and cluster centre. Node analysis is concerned with Non-predictive modelling; each cluster will store information about Destination node, Next hop, Hop count, Destination sequence number, RREP sequence number, Expiration timer, Threshold value, Number of packets [11].

III. Related Work

There are many mitigation and proposed solution for detection and prevention of malicious misbehaviour activity. Our study include strongly emphasized on Onkar V. Chandure [8] who proposed new secure aodv routing algorithm in gray hole attack. Analysis and found problem that it can't take decision and no efficient learning algorithm used for network. We have proposed solution which will take decision and use clustering algorithm to store information, train network and create skew heap tree for each and every node present in network which will insure confidentiality, integrity, availability, authentication and access control. In Ad-hoc network, to make secure AODV, the idea is to understand constraint and find possible mechanism for avoid network threat or detect them. We have analysed and found that AODV uses latest sequence number received by source node towards destination for any route. Hop count which is used for calculate number of hop from source to destination. It is updated so both should be stored in cluster using data mining technique. We proposed solution to take decision based on cluster so we can easily trained our network using learning algorithm.

A. Detection of Attack

We have analysed attributes and major challenges of black hole attack and found that, Attacker used two approaches for disrupt routing process first is not forward packet act as black hole As a result it denies route for communication and second is, in process of route discovery from source to destination, a destination node has to update maximum sequence number in RREQ packet. But malicious node prepares a RREP packet in which increase sequence number

DOI: 03.LSCS.2013.3.35

of destination and convince to source node that it is offer new fresh route with minimum hop count. Source node avoids RREP packet from other node and start communication malicious node route. In flooding attack one particular malicious node continuous floods packet to consume bandwidth. We can detect attack using Threshold value Which will insure sequence number and number of packet generated by node and will train our network to detect attacker.

B. Decision tree

Set theory allows an object to check its degree of membership and form more than one set. Membership function describe, weather our object belongs or doesn't belongs to our set by simple true, false value. Once set membership function defined which will develop decision making capability and form tree structure.

Decision tree contain node where each non-terminal shows test or composite decision based on AND, OR, NOT logic gates. Branches of tree will show result of test upon data sets. We start from root node and follow instruction towards down until reach to terminal (leaf) node. Leaf node labelled with concepts, and having membership function assigned clustering data. Decision tree can form special set rule, observe characteristics of node by hierarchical structure. [10][11]

To create node skew heap data structure we used because it is self-adjusting heap and have ability to merge with logarithmic time. For addition, deletion, and merging time complexity is minimum. So we can easily demonstrate node creation tree structure [9].

IV. Proposed Algorithm

A. Supervised Learning

There are many learning algorithm available in which we proposed supervised learning technique to train network node. Network nodes are label with predefined rules and various classes based training data which is available from data mining algorithm.

Initially in supervised learning accuracy of supervised algorithm deteriorates significantly because large amount of data is not labelled. But using mining algorithm and decision tree it can handle.

We proposed our algorithm and it will start from initialization, in node processing first set waiting time for RREQ and for RREP source node to other neighbour's node, retrieve current time then find response time for each and every node. Additional data object check to find RREP sequence number value is higher than threshold value means node is detect as malicious node and node id store in database and this node will not take process further. Threshold value is depending on sequence number, hop count and number of message, and the end delay. All information was store in GNS clustering. However, the Identity of spurious node or suspected node information will be available in clusters. On this basis data apply supervised learning and will take decision to select proper node. Supervised learning classified node on basis of attack and available information, GNS will support periodically update data object on behaviour of attack. We create tree for selected node process as shown in fig 4.

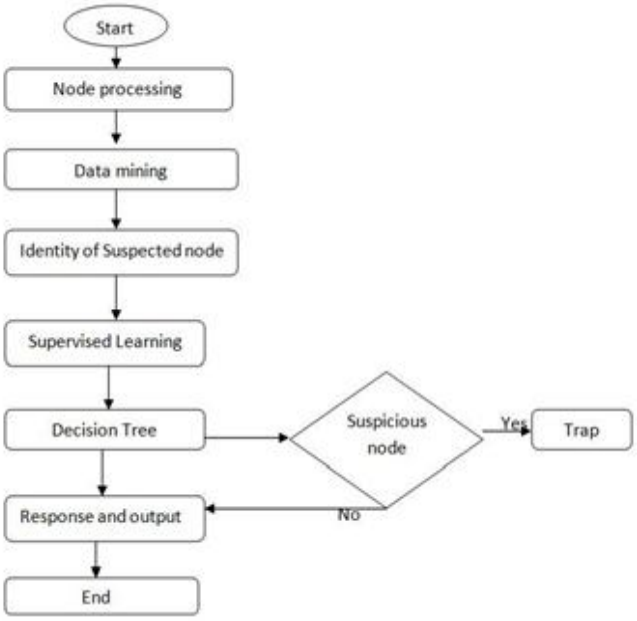

Fig 4: skew Tree for Node Creation

V. Simulation

All attacks which proposed in paper implemented in ns2 and analysis delay, routing overhead packet delivery ratio (PDR) and dropped packet ratio, find out impact on AODV routing algorithm.

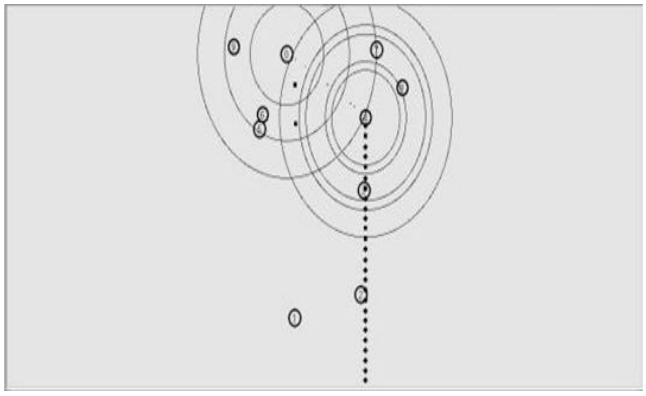

Fig 5: Black hole attack implementation

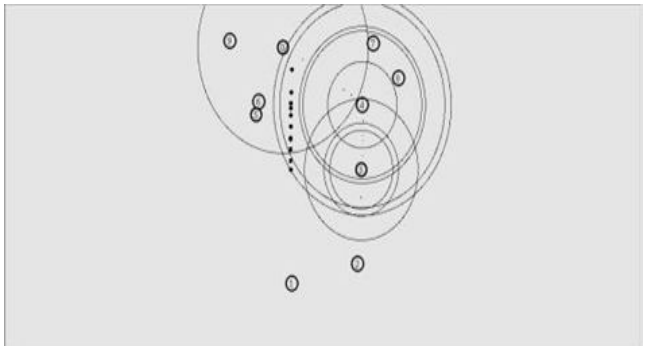

Fig 6: Flooding attack implementation

DOI: 03.LSCS.2013.3.35

Flooding: -
Delay (ms) = 524.00
Routing Overhead (%) = 3.97
PDR = 16.12
Dropped Packet Ratio = 83.89

Black-hole attack: -
Delay (ms)= 517.34
Routing Overhead (%) = 18.05
PDF (or Packet Data Ratio) = 4.11
Dropped Packet Ratio = 95.91

The result shows higher value for the PDR and lower value for the dropped packet ratio for flooding in comparison to Black-Hole attack emphasized on better performance for Flooding in comparison to Black-hole attack. Further we try to design the decision tree for the data obtained from the trace file. The training and testing sample were equally partitioned. The Deviation from the result was very less differed for flooding algorithm in comparison to the black hole attack. Also the overall classification rate very differed slightly in training sample in comparison to testing samples as shown in the Table [1].

TABLE I. CLASSIFICATION FOR THE FLOODING AND BLACK-HOLE ATTACK DATA

Sample	Observed	Predicted	
		opration:9	Percent Correct
Training	opration:0	9	99.7%
	opration:1	1	.0%
	opration:2	0	38.5%
	opration:3	1	.0%
	opration:4	1	42.0%
	opration:5	11	17.0%
	opration:6	10	40.6%
	opration:8	1	40.6%
	opration:9	14	25.0%
	Overall Percentage	.2%	78.0%
Test	opration:0	13	99.7%
	opration:1	1	.0%
	opration:2	0	39.6%
	opration:3	1	.0%
	opration:4	3	43.9%
	opration:5	13	17.0%
	opration:6	12	40.8%
	opration:8	1	40.7%
	opration:9	8	13.8%
	Overall Percentage	.2%	78.0%

Growing Method: CHAID
Dependent Variable: opration:4

VI. CONCLUSION

Ad-hoc network require less complex efficient, reliable, highly secure routing protocol because it contain self-organize in- secure dynamic topology in which nodes are continuous changing its position. AODV is vulnerable to Route discovery in black hole, gray hole, and flooding attacks. Therefore we discussed techniques for detection and prevention of attacks and take decision using learning to make more secure AODV routing algorithm. The further work can be discussed by considering the various node structures so to compare the performance of each with respect to the Packet drop rate and packet data rate.

REFERENCES

[1] Sarkar S. K., Ad hoc mobile wireless network Chapter 1, Auerbach publications September 2011.
[2] Lidong Z., Securing Ad Hoc Networks, Cornell University, IEEE network, special issue on network security, November/ December, 1999.
[3] Patidar V., Black Hole Attack and its Counter Measures in AODV Routing Protocol, IJCER, Vol. 2, Issue-5 September 2012.
[4] Chandure O., Detection & Prevention of GRAY Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol, IJOCA Volume 41–No.5, 2012.
[5] Molsa J., Mitigating denial of service attacks, Journal of Computer Security 13 (2005).
[6] Rutvij H., Jhaveri M., routing MANET protocols and wormhole attack against AODV, IJCSNS, VOL.10 No.4, April 2010.
[7] Depa P., pattern recognition for cluster identification problem, Special Issue of International Journal of Computer Science & Informatics **(**IJCSI) Nov, 2012.
[8] Chandure O.V., Simulation of secure AODV in GRAY hole attack for mobile ad-hoc network, IJAET, Nov. 2012.
[9] Daniel Dominic Sleator and Robert Endre Tarjan, Self-Adjusting Heaps, 02 August 2006.
[10] Smith F. James, naval Research laboratory, fuzzy logic resource manager evolving fuzzy decision tree structure adapt in real time. Proceedings of the Sixth International Conference of Information Fusion - FUSION 2003, Volume: 2.
[11] Joshi Manish, Amity University, classification, clustering, and intrusion detection system, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.961-964
[12]Yadav H., A Review on black hole attack in MANET, IJERA, ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012.

DOI: 03.LSCS.2013.3.35